

# Changing Conceptions of Privacy

by Maria Dailey & M. E. Kabay, PhD, CISSP-ISSMP  
School of Business & Management  
Norwich University, Northfield VT

*Maria Dailey is a senior in the Bachelor of Science in Computer Security and Information Assurance (BSCSIA) in the School of Business at Norwich University. She recently submitted an interesting essay in the IS455 Strategic Applications of Information Technology < <http://www.mekabay.com/courses/academic/norwich/is455/index.htm> > course, and I suggested to her that we work together to edit and expand it for publication. The following is the result of a close collaboration between us.*

\* \* \*

## NTHNTF?

Privacy opponents feel that there is no need for privacy. If there is nothing to hide, there exists no real excuse to hide information. That belief is often described as the nothing-to-hide-nothing-to-fear (NTHNTF) position. In an extreme statement of this position, former *News of the World* deputy features editor Paul McMullan, speaking before the Leveson inquiry[1], said,

“In 21 years of invading people's privacy I've never actually come across anyone who's been doing any good. Privacy is the space bad people need to do bad things in. Privacy is for paedos. If there is a privacy law your secrets are going to be much more valuable than they were before.”[2]

Those opposed to NTHNTF belief argue that certain information taken out of context can result in undeserved consequences to innocent citizens. “Privacy protects us from being misdefined and judged out of context in a world...in which information can easily be confused with knowledge.”[3]

The *Privacy, Identity & Consent Blog*[4] author, Toby Stevens,[5] summarizes current developments in privacy law and policy; in one posting at the end of 2010, he articulates his concerns about the effects of the Internet on privacy:

“In 1890, Samuel Warren and Louis Brandeis famously described privacy as “the right to be let alone.” For over a century since then, society has developed legal, technical and social frameworks that protected a concept of alone-ness, of isolation, of keeping others away from the individual and information about that individual. Our concept of privacy has become one of ‘urban anonymity.’ we believe we have some degree of anonymity when we are in public, since if nobody knows who we are, then our actions cannot have consequences since we can’t be identified.

But ... the emergence of the Internet has stood that idea on its head in the past ten years. The explosion of data, of access to that data, of tools to search, filter, analyse, interrogate, present and disseminate that data, placed in the hands of government, companies and individuals have stripped away that veneer of anonymity and created a dystopia in which our privacy is fading, not because of our failure to control privacy, but because privacy itself has changed, and the old controls are no longer able to contain or to manage the ways in which we share information with others....

Privacy is no longer about keeping our personal information secret, but is instead about controlling how it is used. And unless we can enforce that control, the only possible outcome for our society is total transparency: a world in which nobody has any secrets at all, and individuals have no meaningful control over how those secrets are used. Nothing is ignored, nothing is forgotten, nothing is forgiven...."[6]

### **Radically Increased Access**

One of the developing features of information technology is how much information one can find about another person. White Pages on Yellowpages.com permits any user to look up the current telephone and address of anyone within the United States, as long as the individual searched for is listed.[7] Although this is a digital version of a paper book most people receive at home, it provides a wider pool of both searchers and targets, no longer limiting them to a common area – or increasing the common area to the entire nation.

Other Websites, such as MyLife.com, provide more detailed information on specific individuals to anyone who has signed up and chosen an inexpensive membership. Anyone can join and acquire as much information as he or she desires. MyLife “helps you find people from anytime in your life, no matter where they are,” and aims to “provide the most comprehensive people search service.” MyLife provides information on over 750 million people by collecting publicly available information, and has a feature enabling anyone with a paid account to see who is searching for him or her. [8] This “publicly available information” is extensive, and reaches further when individuals do not protect information they wish to remain exclusively available to certain people.

Electronic searches may increase the susceptibility to crime. In a recent summary, Mark Jenkins of Channel 13 News in Orlando, Florida warned that social-media users should not post detailed information about their vacation plans: “...[T]hanks to social networks, criminals can tell the moment you leave your home and how long you’re gone. They'd have easy access to your vacant home.” He quoted a police officer with specific advice:

Corporal Marcus Camacho with the Orange County Sheriff’s Office said it's a major travel mistake. “[With] Smart phones, today, you can update your location so anybody could know where you’re at, at any time,” Camacho said. “What they don't realize is people are seeing that. Especially if you have a public view on your social networking site that everybody can see that.”[9]

*Google Earth* can provide photographs of many addresses from street level.[10] Shortly after it was introduced, there was a flurry of concerns about the effects of street-level, detailed photographs on privacy; for example, *TIME Magazine* writer S. James Snyder wrote in 2007,

“Google's new “Street View” has sent techies scrambling to browse through the miles and miles of street-level photos now available through Google Maps. But while such blogs as BoingBoing.net and Mashable.com have made something of a joke out of the many humorous (a man apparently caught mid-sneeze), bizarre (the ghost of E.T.?) and lewd (a woman's underwear poking out of her low-riding jeans) images captured by the web giant, privacy concerns have led many watchdog groups to quickly retort that Street View is no laughing matter.”[11]

Google responded quickly, publishing a privacy page about street-level *Google earth*. Among the privacy protections outlined are

- Photographs are from public access only;
- The images can be several months old;
- Individuals and license plates are automatically blurred;
- Anyone can request additional blurring of details or removal of images containing objectionable material such as nudity or violence.

## Concluding Remarks

Changing communications technology has already begun to change the nature of privacy. Users of the Web and related services should think about the implications of public disclosure of information and filter their postings with what may become *common sense* in a generation or so but is to date definitely still *uncommon* sense.

*In the next posting, Maria and Mich will discuss privacy implications of recent controversies over social networking sites and privacy.*

## References

- [1] Guardian 2011
- [2] Halliday and O'Carroll 2011
- [3] Privacy Rights Clearinghouse 2011
- [4] Stevens, Privacy, Identity & Consent: The Data Trust Blog 2011
- [5] Enterprise Privacy Group 2011
- [6] Stevens, Private Lives in a Database World 2010
- [7] AT&T 2011
- [8] MyLife.com Inc 2011
- [9] Jenkins 2011
- [10] Google 2011
- [11] Snyder 2007

## Works Cited

- AT&T. *White Pages*. 2011. <http://www.yellowpages.com/whitepages> (accessed 11 24, 2011).
- Enterprise Privacy Group. "Company Profile: The EPG Team." *Enterprise Privacy Group*. 2011. <http://www.privacygroup.org/content/view/18/23/> (accessed 12 24, 2011).
- Google. *Google earth*. 2011. <http://www.google.com/earth/index.html> (accessed 12 24, 2011).
- Guardian. *Leveson inquiry*. 12 2011. <http://www.guardian.co.uk/media/leveson-inquiry> (accessed 12 24, 2011).
- Halliday, Josh, and Lisa O'Carroll. *Rebekah Brooks and Andy Coulson are 'scum of journalism', Leveson told*. 29 11 2011. <http://www.guardian.co.uk/media/2011/nov/29/rebekah-brooks-andy-coulson-leveson-inquiry> (accessed 12 24, 2011).
- Jenkins, Mark. "You may be leading burglars to your house with online posts." *Central Florida News 13*. 23 12 2011. <http://www.cfnews13.com/article/news/2011/december/360770/You-may-be-leading-burglars-to-your-house-with-online-posts> (accessed 12 23, 2011).
- MyLife.com Inc. "About US." *MyLife*. 2011. <http://www.mylife.com/aboutUs.pub> (accessed 12 24, 2011).
- Privacy Rights Clearinghouse. *Privacy Today: A Review of Current Issues*. 1 March 2011. <https://www.privacyrights.org/ar/Privacy-IssuesList.htm#dataprofiling> (accessed 11 30, 2011).
- Snyder, S. James. "Google Maps: An Invasion of Privacy?" *TIME Business*. 12 06 2007. <http://www.time.com/time/business/article/0,8599,1631957,00.html> (accessed 12 24, 2011).
- Stevens, Toby. *Privacy, Identity & Consent: The Data Trust Blog*. 24 08 2011. <http://www.computerweekly.com/blogs/the-data-trust-blog/> (accessed 12 23, 2011).
- . "Private Lives in a Database World." *Privacy, Identity & Consent: The Data Trust Blog*. 07 12 2010. <http://www.computerweekly.com/blogs/the-data-trust-blog/2010/12/private-lives-in-a-database-wo.html> (accessed 12 24, 2011).

\* \* \*

M. E. Kabay, <<mailto:mekabay@gmail.com>> PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials. <<http://www.mekabay.com/>>

\* \* \*

Copyright © 2012 Maria Dailey & M. E. Kabay. All rights reserved.